



UNITED STATES PATENT AND TRADEMARK OFFICE

mn
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|---------------------|------------------|
| 10/813,927 | 03/31/2004 | Bernard Plessier | 851663.467 | 5064 |
| 38106 | 7590 | 08/03/2007 | EXAMINER | |
| SEED INTELLECTUAL PROPERTY LAW GROUP PLLC 701 FIFTH AVENUE, SUITE 5400 SEATTLE, WA 98104-7092 | | | DO, CHAT C | |
| | | ART UNIT | PAPER NUMBER | |
| | | 2193 | | |
| | | MAIL DATE | DELIVERY MODE | |
| | | 08/03/2007 | PAPER | |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

| | | | |
|------------------------------|------------------------|---------------------|--|
| Office Action Summary | Application No. | Applicant(s) | |
| | 10/813,927 | PLESSIER, BERNARD | |
| | Examiner | Art Unit | |
| | Chat C. Do | 2193 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 31 March 2004 and 13 August 2004.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-15 is/are pending in the application.
- 4a) Of the above claim(s) 7-11 is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-6 and 12-15 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 31 March 2004 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. attached herein.
- 5) Notice of Informal Patent Application
- 6) Other: _____.

DETAILED ACTION

Election/Restrictions

1. This application contains claims directed to the following patentably distinct species:

Species I: claims 1-6 and 12-15 direct to an apparatus for performing modular operation utilizing 2-CSA and 1-CSA in series.

Species II: claims 7-11 direct to a method and apparatus for performing modular operation including to set the result (S) to specific conditions.

The species are independent or distinct because the apparatus of species I does not need specific setting of the result (S) and specific structure of utilizing AND gate in apparatus wherein species II does not need specific inputs as seen in species I.

Applicant is required under 35 U.S.C. 121 to elect a single disclosed species for prosecution on the merits to which the claims shall be restricted if no generic claim is finally held to be allowable. Currently, there is no generic.

Applicant is advised that a reply to this requirement must include an identification of the species that is elected consonant with this requirement, and a listing of all claims readable thereon, including any claims subsequently added. An argument that a claim is allowable or that all claims are generic is considered nonresponsive unless accompanied by an election.

Upon the allowance of a generic claim, applicant will be entitled to consideration of claims to additional species which depend from or otherwise require all the limitations of an allowable generic claim as provided by 37 CFR 1.141. If claims are added after the election, applicant must indicate which are readable upon the elected species. MPEP § 809.02(a).

2. During a telephone conversation with the attorney of record, E. Russell Tarleton Reg. No. 31,800 on 07/16/2007 a provisional election was made without traverse to prosecute the invention of Group I, claims 1-6 and 12-15. Affirmation of this election must be made by applicant in replying to this Office action. Claims 7-11 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Specification

3. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

4. The abstract of the disclosure is objected to because the abstract is written less than 150 words in length and there is an extra line right below the abstract paragraph. Correction is required. See MPEP § 608.01(b).

Claim Objections

5. Claims 2 and 4 are objected to because of the following informalities:

Re claim 2, the applicant is advised to re-write the term “Result” as “result” in line 2 unless it refers to some other result that is differ from previous result (R). Claim 4 also has the same objection.

Re claim 4, the applicant is advised to re-write the term “LSB” as “least significant bit” for clarification issue.

For general claims, the applicant is advised to use subscript for current iteration if possible. In addition, the applicant is advised to use asterisk (*) as multiplication sign instead of period (.) or blank () as multiplication sign.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-6 and 12-15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Re claim 1, the parameter “ Y_0 ” in line 6 is unclear of what it is. Further, limitation “ U_3 , being $S/2$ ” in line 11 is mis-descriptive since S is unknown as we are computing. For examination purposes, the examiner considers U_3 , being $(S_{i-1} * (t-p))/2$ as seen in Figure 4. Further, the limitation “ $J_0 N <0> = -1 \bmod 2^p$ ” in line 16 is unclear whether it is as $J_0 * N_0 = -1 \bmod 2^p$ or both $(J_0 * N)$ and $(-1 \bmod 2^p)$ are less than zero.

For examination purposes, the examiner considers the limitation “ $J_0N<0>=-1 \text{ mod } 2^p$ ” as $J_0 * N_0 = -1 \text{ mod } 2^p$. Claim 12 has similar rejection.

Re claim 4, the limitation “while processing bits 0 to $p-1$ ” is unclear of its reference because it does not clearly disclose the processing bits belong to A, B, S, or N. For examination purposes, the examiner considers the processing bits 0 to $p-1$ of input A as it is divided into sub-block for processing.

Thus, claims 2-3, 5-6, and 13-15 are rejected for being dependent on the rejected base claims 1 and 12.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. Claims 1-6 and 12-15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-6 and 12-15 cite an apparatus for performing Montgomery modular calculation in accordance with a mathematical algorithm. In order for claims to be statutory, claims must either include a practical/physical application or a concrete, useful, and tangible result. However, claims 1-6 and 12-15 merely disclose steps/components for performing Montgomery modular calculation without further disclosing a practical/physical application or a useful and tangible result since the claims appear to preempt every substantial practical application of the idea embodied by the claim and

there is no cited limitation in the claims that breathes sufficient life and meaning into the preamble so as to limit it to a particular practical application rather than being so broad and sweeping as to cover every substantial practical application of the idea embodied therein. Therefore, claims 1-6 and 12-15 are directed to non-statutory subject matter.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. U.S. Patent No. 6,275,837 to Plessier discloses a method for the implementation of an elementary modular operation according to the Montgomery method.
- b. U.S. Patent Application Publication No. 2004/0267855 to Shantz et al. disclose a method and apparatus for implementing processor instructions for accelerating public-key cryptography.
- c. U.S. Patent Application Publication No. 2004/0179681 to Lee et al. disclose an apparatus and method for performing Montgomery type modular multiplication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chat C. Do whose telephone number is (571) 272-3721. The examiner can normally be reached on M => F from 7:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An can be reached on (571) 272-3756. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2193

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Chat C. Do
Examiner
Art Unit 2193

July 25, 2007

A handwritten signature in black ink, appearing to read "Chat C. Do".